Submitted by: Aryan Raj, Roll No.- 170123010

Question 1: a) '**ping -c count**' option required to specify the number of echo requests to send with ping.

b) '**ping -i interval**' option required to set time interval (in seconds), rather than the default 'one' second interval, between two successive ping ECHO_REQUESTs. Normal users cannot set interval to values less than 0.2 seconds except super-users.

c) '**ping -l preload**' is the command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply. The limit for sending such ECHO_REQUEST packets by normal users (not super user) is 3.

d) '**ping-s packetsize**' command to set the ECHO_REQUEST packet size (in bytes). The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
If the packetsize is set to 32 bytes, the total packetsize will be 40 bytes as 8 bytes of ICMP header data is added to the 32 bytes i.e. (32+8) bytes.

Question 2: Following table shows average RTT for all hosts at three different hours of the day (using "spfld.com/ping.html"):

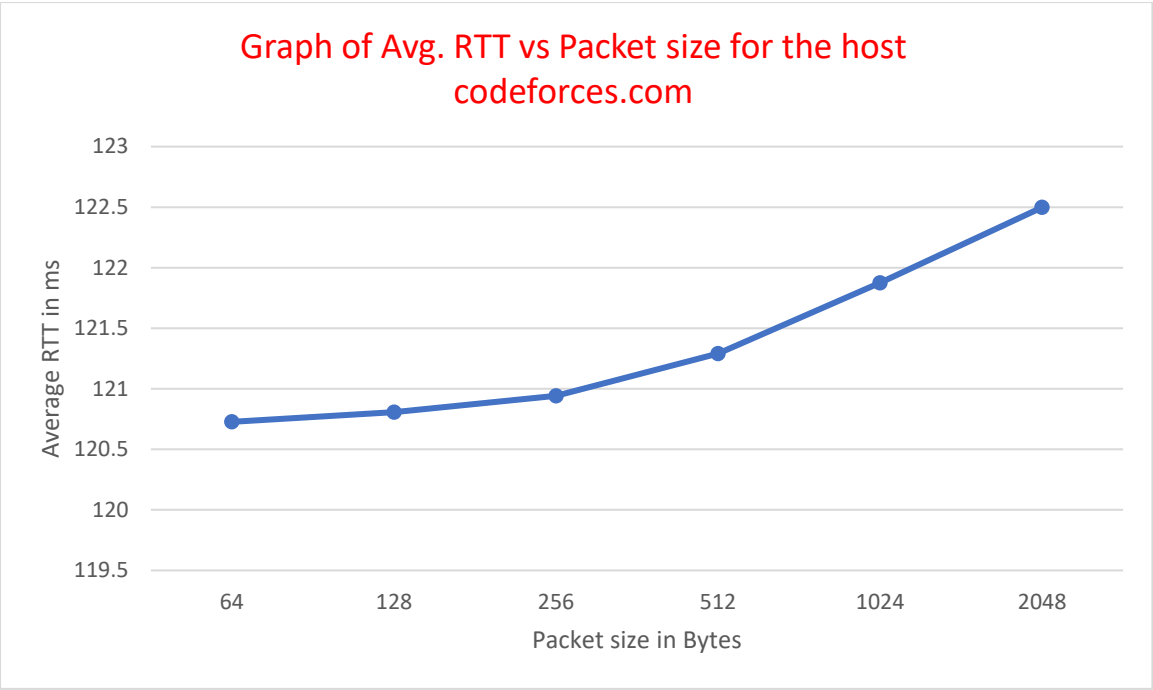
Host Name	Average RTT (18 Jan,11 PM) in ms Average	Average RTT (18 Jan,08 AM) in ms Average	Average RTT (18 Jan,04 PM) in ms Average	Overall Average RTT in ms	Percentage packet loss
google.com	40.103	40.214	40.071	40.129	0
facebook.com	23.190	22.948	22.656	22.931	0
flipkart.com	242.569	243.495	242.763	242.942	0
cricbuzz.com	281.983	279.758	282.668	281.470	0
hotmail.com	No RTT	No RTT	No RTT	N/A	100
codeforces.com	121.939	122.219	121.665	121.941	0

Yes, there exists a case where packet loss is more than 0% i.e. hotmail.com shows 100% packet loss. There are many possible reasons. There could be restrictions on the source IP address that can be accessed. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination, which can be because the firewall is blocking. It is also possible that there is some network congestion or target IP address might not have any network device connected with it.

There exists a weak positive correlation between distance (the geographical location of the hosts) and RTT. All the six selected hosts are very close to each another in terms of geographical location whereas the RTT are too scattered. Mainly it will depend on how many routers/switches come into way, as transmission will not take much time. At each router there may be a delay, so if the packets have to go through more distance, thus more routers, therefore longer the RTT. However, Geographical distance b/n two hosts does not directly give the path through which the packet travels.

I picked codeforces.com and experimented with different packet sizes ranging from 64-bytes to 2048-bytes.

Packet Size(in Bytes)	64	128	256	512	1024	2048
Average RTT(in ms)	120.727	120.806	120.943	121.290	121.875	122.498



Note - It is possible that there is packet loss of 100% for some site while using packet size 2048 bytes if the frame size exceeds the MTU size of the interface (i.e. 1500 in this case). Using fragmentation, the host can send ECHO REQUESTS for this packet size.

With increase in packet size, RTT increases as shown in the above figure. Time influence on RTT measurements can be understood as different hours correspond to different busy working hours of different continents. For ex- Higher RTT can be observed during daytime in India while lower RTT is observed post sunset.

Question 3: IP chosen: 172.17.0.23 (intranet.iitg.ac.in)

a) The packet loss rate for command:
ping -n 172.17.0.23 is 0.1% (i.e. 1 out of 1000 packets is lost)
ping -p ff00 172.17.0.23 is 0.2% (i.e. 2 out of 1000 packets are lost)

b) The following tables can be used to visualize the different kinds of latencies for both the commands:

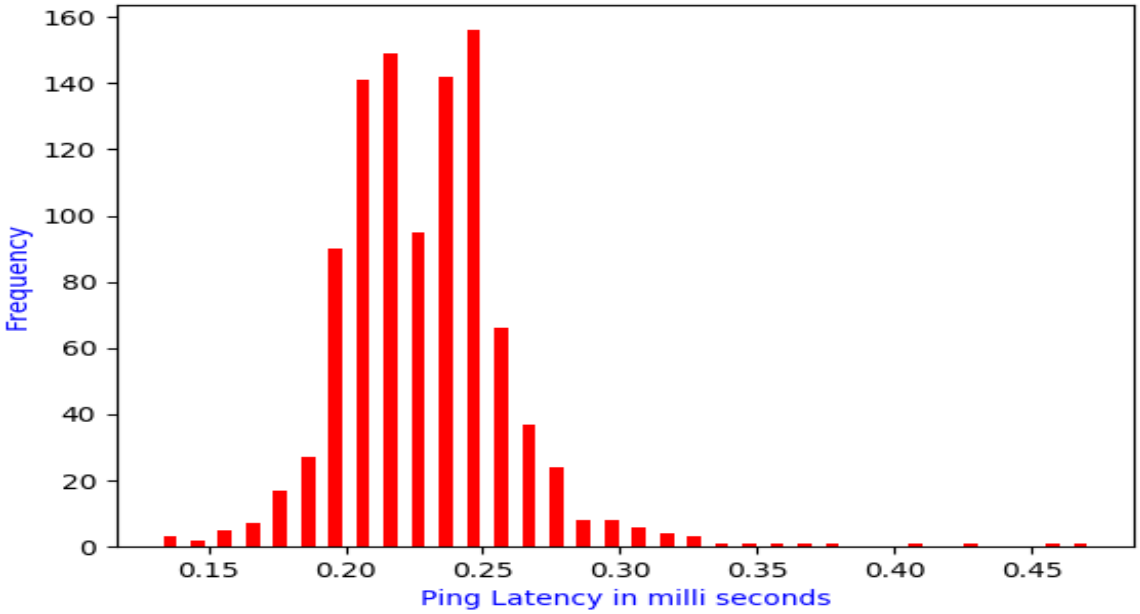
Minimum Latency	Maximum Latency	Mean Latency	Median Latency
0.117	0.423	0.229	0.228

Table for command “ping -n 172.17.0.23”

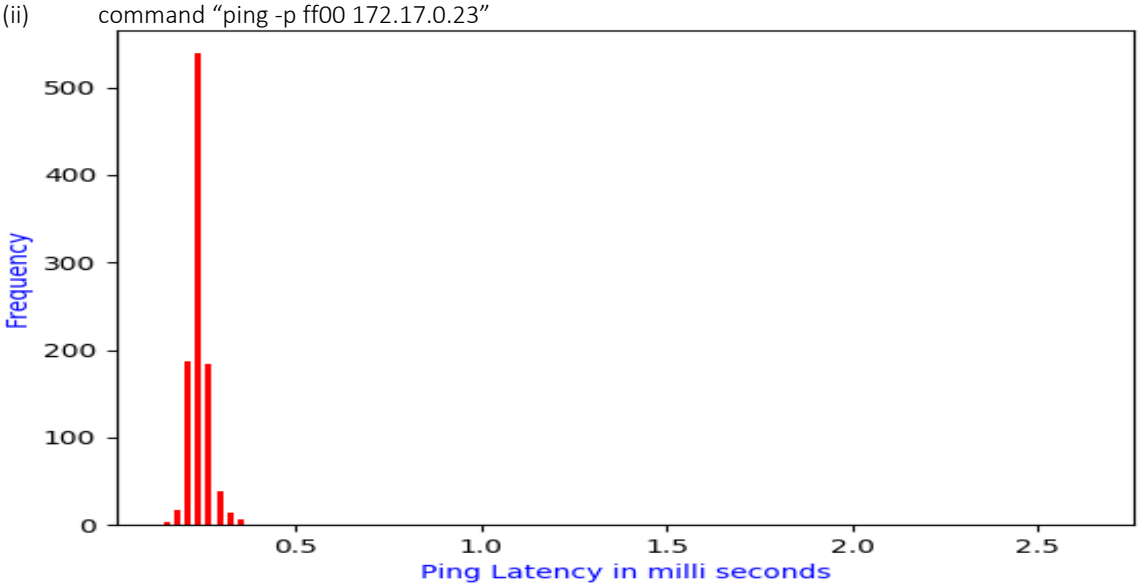
Minimum Latency	Maximum Latency	Mean Latency	Median Latency
0.118	1.576	0.246	0.241

Table for command “ping -p ff00 172.17.0.23”

c) The normal distribution for the two cases is as follows:
(i) command “ping -n 172.17.0.23”:-



(ii) command “ping -p ff00 172.17.0.23”



d) For ping -n 1000 172.17.0.23, the RTT values lied b/w 0.117 and 0.423 as can be visualized from the table. There was a packet loss of 0.1% i.e. 1 out of the 1000 packets lost, 999 of them were received back successfully.
For ping -p ff00 172.17.0.23, the RTT values lie b/w 0.118 and 1.576. A histogram was used to represent the latencies using this command. There was a packet loss of 0.2% in this case i.e. out of the 1000 packets sent, 998 of them were received back successfully.
The standard deviation for ping -n was found to be 0.034 while that for ping -p was found to be 0.1. ping -n carries the default pattern whereas ping -p carries the given i/p pattern.

Question 4:

a) **Ifconfig** (interface configuration) is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface. If no arguments are given, ifconfig displays the status of the currently active interfaces.

```
aryan@world-of-aryan:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.3.3.61  netmask 255.255.252.0  broadcast 10.3.3.255
        inet6 fe80::f68e:38ff:fef3:a551  prefixlen 64  scopeid 0x20<link>
        ether f4:8e:38:f3:a5:51  txqueuelen 1000  (Ethernet)
        RX packets 21691  bytes 1692718 (1.6 MB)
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 24724  bytes 2101937 (2.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 305  bytes 25623 (25.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 305  bytes 25623 (25.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Analysis & Explanation of Terminologies in the output of ifconfig:

Here enp2s0, lo are the names of the active network interfaces on the system.

1) **enp2s0** is the first Ethernet interface. Subsequent Ethernet interfaces would be named enp2s1, enp2s2, etc.

2) **lo** is the loopback interface. This is a special network interface, which the system uses to communicate with itself.

ether f4:8e:38:f3:a5:51 – This is the hardware address or MAC address which is unique to each Ethernet card which is manufactured. First part is manufacturers' code and second part is the device id.

txqueuelen: 1000: This denotes the length of the transmit queue of the device.

inet : Indicates the machine IP address

netmask – is the network mask which we passed using the netmask option

inet6: IPV6 address of the interface.

UP: This flag indicates that the kernel modules related to the Ethernet interface has been loaded.

BROADCAST: Denotes that the Ethernet device supports broadcasting- a necessary characteristic to obtain IP address via DHCP.

RUNNING: The interface is ready to accept data.

MULTICAST: This indicates that the Ethernet interface supports multicasting.

mtu 1500:(Maximum Transmission Unit)- This is the size of each packet received by the Ethernet card. The value of MTU for all Ethernet devices by default is set to 1500.

RX packets, TX packets – This shows the total number of packets received and transmitted respectively. It includes:

(i) **Errors**: Number of damaged packets received/transmitted.

(ii) **Dropped**: Number of dropped packets due to reception errors.

(iii) **Overruns**: Number of received/transmitted packets that experienced data overruns.

(iv) **Frame**: Number of received packets that experienced frame errors. Parameter has significance only while routing packets.

(v) **Carrier**: Number received packets that experienced loss of carriers.

(vi) **collisions: 0**: The value of this field should ideally be 0. If it has a value greater than zero, it could mean that the packets are colliding while traversing your network i.e. sign of network congestion.

RX Bytes, TX Bytes- These indicate the total amount of data that has passed through the interface.

b) Options that can be provided with the ifconfig command:-

(i) '**-a**'- to display all interfaces which are currently available, even if down.

(ii) '**-v**'- used to be more verbose for some error conditions.

(iii) '**-s**'- to display a short list.

(iv) interface: The name of the interface. This is usually a driver name followed by a unit number, for example eth0.

(v) '**up**'- This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface; we can suppress this behaviour when using an alias interface by appending an- to the alias (e.g. eth0:0-). It is also suppressed when using the IPv4 0.0.0.0 address as the kernel will use this to implicitly delete alias interfaces.

(vi) '**down**'- This flag causes the driver for this interface to be shut down.

(vii) '**arp**'- Enable or disable the use of the ARP protocol on this interface.

(viii) '**promisc**'- Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.

c)

```
aryan@world-of-aryan:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

Route command is used to view and manipulate the IP routing tables in both UNIX and Windows based systems. Running route at the command line without any options displays the routing table entries. This shows us how the system is currently configured and existing routes table. If a packet comes into the system and has a destination in the range 10.3.0.0 through 10.3.0.255, then it is forwarded to the gateway 0.0.0.0 — A special address which represents an invalid or non-existing destination.
If the destination is not in this IP address range, it is forwarded to the default gateway here 10.3.0.254 and that system will determine how to forward the traffic on to the next step towards its destination.
d)

```
aryan@world-of-aryan:~$ route -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

'**route -F'** - operate on the kernel's FIB (Forwarding Information Base) routing table. This is the default.

```
aryan@world-of-aryan:~$ sudo route add -net 127.0.0.0 netmask 255.0.0.0 metric 1024 dev lo
aryan@world-of-aryan:~$ sudo route add -net 192.168.0.0 netmask 255.255.255.0 dev enp2s0
aryan@world-of-aryan:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
127.0.0.0       0.0.0.0         255.0.0.0       U     1024   0        0 lo
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 enp2s0
aryan@world-of-aryan:~$ sudo route del -net 192.168.0.0 netmask 255.255.255.0
aryan@world-of-aryan:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
127.0.0.0       0.0.0.0         255.0.0.0       U     1024   0        0 lo
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

route add – Adds a new route.
netmask – When adding a network route, netmask to be used.
metric – Sets the metric field in the routing table.
dev – Forces the route to be associated with a particular device.
route del – Deletes a route.

```
aryan@world-of-aryan:~$ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U         0 0          0 enp2s0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp2s0
aryan@world-of-aryan:~$
aryan@world-of-aryan:~$ route --cache
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
aryan@world-of-aryan:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.3.0.254      0.0.0.0         UG    20100  0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
127.0.0.0       0.0.0.0         255.0.0.0       U     1024   0        0 lo
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

route -e – Uses netstat format for displaying the routing table.
route -C / route --cache – Operates on the kernel's routing cache.
route -n – Shows numerical addresses instead of symbolic hostnames.

Question 5:

a) **netstat** provides information and statistics about protocols in use and current TCP/IP network connections. It is used for finding problems in the network, to determine the amount of traffic on the network as a performance measurement and for checking our network configuration and activity.
b) We use the command '**netstat-t | grep-e ESTABLISHED-e state'** to list all the established TCP connections as can be seen from the below image.

```
aryan@world-of-aryan:~$ netstat -t | grep -e ESTABLISHED -e state
tcp        0      0 world-of-aryan:48078    xx-fbcdn-shv-02-b:https ESTABLISHED
tcp        0      0 world-of-aryan:39868    maa05s01-in-f10.1:https ESTABLISHED
tcp        0      0 world-of-aryan:50164    maa05s05-in-f1.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:51296    maa03s20-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:35964    maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:53914    maa05s10-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:58784    maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:50158    maa05s05-in-f1.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:36984    maa05s01-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:46132    e2a.google.com:https    ESTABLISHED
tcp        0      0 world-of-aryan:45422    104.24.108.176:https    ESTABLISHED
tcp        0      0 world-of-aryan:40928    pkt-nrt-k1-shared:https ESTABLISHED
tcp        0      0 world-of-aryan:48056    xx-fbcdn-shv-02-b:https ESTABLISHED
tcp        0      0 world-of-aryan:60248    maa05s03-in-f8.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:37638    maa03s31-in-f13.1:https ESTABLISHED
tcp        0      0 world-of-aryan:37574    maa05s10-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:41570    maa05s06-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:38010    maa03s29-in-f22.1:https ESTABLISHED
tcp        0      0 world-of-aryan:35406    52.114.88.28:https      ESTABLISHED
tcp        0      0 world-of-aryan:41354    maa03s29-in-f1.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:50676    ec2-52-21-96-229.:https ESTABLISHED
tcp        0      0 world-of-aryan:37586    maa05s10-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:41180    maa05s04-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:57566    a23-1-37-126.depl:https ESTABLISHED
tcp        0      0 world-of-aryan:53964    maa05s10-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:55244    147.75.94.109:https     ESTABLISHED
tcp        0      0 world-of-aryan:35400    52.114.88.28:https      ESTABLISHED
tcp        0      0 world-of-aryan:48864    maa03s28-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:43118    maa05s09-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:58666    maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:42930    maa03s26-in-f10.1:https ESTABLISHED
tcp        0      0 world-of-aryan:40942    pkt-nrt-k1-shared:https ESTABLISHED
tcp        0      0 world-of-aryan:58708    maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:50806    maa05s01-in-f8.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:42168    maa03s26-in-f14.1:https ESTABLISHED
tcp        0      0 world-of-aryan:54204    13.107.18.11:https      ESTABLISHED
tcp        0      0 world-of-aryan:54422    maa03s31-in-f4.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:49680    52.109.124.84:https     ESTABLISHED
tcp        0      0 world-of-aryan:50048    13.107.3.128:https      ESTABLISHED
tcp        0      0 world-of-aryan:60202    180.149.52.83:https     ESTABLISHED
tcp        0      0 world-of-aryan:40562    maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 world-of-aryan:47014    edge-star-mini-sh:https ESTABLISHED
```

The fields are:

- **Proto**: The name of the protocol used by the socket which is tcp in this case.
- **Recv-Q**: The count of bytes not copied by the user program connected to this socket.
- **Send-Q**: The count of bytes yet to be acknowledged by the remote host.
- **Local address**: Address and port number of the local end of the socket.
- **Foreign address**: Address and port number of the remote end of the socket.
- **State**: The state of the socket connected in b/w the Local Address and Foreign Address. These states represent the three-way handshake communication system that TCP uses.

c)

```
aryan@world-of-aryan:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U         0 0          0 enp2s0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp2s0
```

netstat-r is used to get the kernel routing information. The fields are:

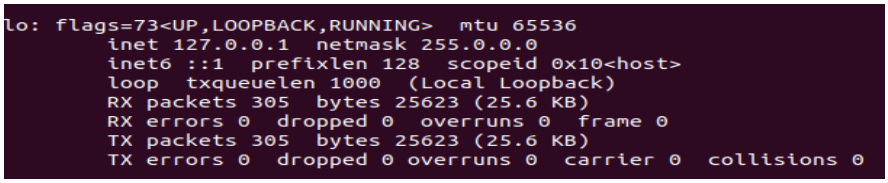
- **Destination**: The destination network or destination host.
- **Gateway**: The gateway to which the routing entry points.
- **Genmask**: The netmask for the destination net; 0.0.0.0 for default route.
- **Flags**: This signifies route is up to gateway or host.
- **MSS**: Default maximum segment size for TCP connection over route.
- **Window**: Default window size over this route.
- **irtt**: Initial RTT (Round Trip Time).
- **Iface**: Interface to which packets for this route will be sent.

d) **netstat -i** can be used to display the status of all network interfaces. netstat -I | wc -l can be used to figure out the number of interfaces on PC.

e) **netstat-su** can be used to show the statistics of all the UDP connections.

```
aryan@world-of-aryan:~$ netstat -su
IcmpMsg:
    InType0: 30
    InType3: 38
    InType8: 10
    OutType0: 10
    OutType3: 37
    OutType8: 54
Udp:
    15997 packets received
    1 packets to unknown port received
    0 packet receive errors
    1420 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
IpExt:
    InMcastPkts: 8913
    OutMcastPkts: 139
    InBcastPkts: 5587
    OutBcastPkts: 1
    InOctets: 1235467242
    OutOctets: 22386730
    InMcastOctets: 889569
    OutMcastOctets: 21433
    InBcastOctets: 1003354
    OutBcastOctets: 65
    InNoECTPkts: 853134
```

f) The **loopback** device is a special, virtual network interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. It is the very first interface to be activated. The role of a Loopback Interface comes when a network interface is disconnected--for example, when an Ethernet port is unplugged or Wi-Fi is turned off or not associated with an access point--no communication on that interface is possible, not even communication between your computer and itself.



Question 6: Used http://network-tools.com tool and six hosts of my choice for traceroute experiment:

Host Name	Hop Count (11 AM)	Hop Count (5 PM)	Hop Count (11 PM)
google.com	7	7	7
facebook.com	8	9	8
flipkart.com	10	10	10
cricbuzz.com	25	25	25
codeforces.com	11 (Firewall Reached)	11 (Firewall Reached)	11 (Firewall Reached)
hotmail.com	5 (Firewall Reached)	5 (Firewall Reached)	5 (Firewall Reached)

The common hops of the six hosts are as follows:

Host Name	Common Hops (IP Address)
google.com	91.194.90.1, 93.104.204.33, 212.18.6.109, 93.104.240.55 (4 in total)
facebook.com	91.194.90.1, 157.240.38.155 (2 in total)
flipkart.com	91.194.90.1,163.53.78.128,91.194.90.1,213.248.101.77,213.248.82.41,195.219.194.149 (9 in total)
cricbuzz.com	91.194.90.1, 93.104.204.33,93.104.240.55 (7 in total)
codeforces.com	91.194.90.1,212.78.183.245,212.74.66.225 (9 in total)
hotmail.com	91.194.90.1, 213.248.101.77, 62.115.120.119, 62.115.112.199, 62.115.14.10 (5 in total)

b) Yes, route to same host can change at different times of the day. This may be because destination host utilizes multiple Internet servers to handle incoming requests, so it shows different IP addresses. There is fast switching with which after a packet was sent to the next hop, the routing information about how to get to the destination is stored in a fast cache. When the router receives another packet that is directed to the same destination it uses the cache. Therefore, some router's IP are selected from the routing table, which was used earlier and now is found to be inactive then another router IP will be selected.

c) Yes, traceroute for hotmail.com did not find complete paths to the hosts as it shows trace aborted at the end. Traceroute is unable to find complete paths to some host because Firewall of that host might be blocking our IP, or we need to increase max hops, as packets might not reach to destination within fixed max hops. Other reason may be packet loss between various routers in between the path.

d) Yes, it is possible that tracerouting to certain hosts may be possible even though same host fail to respond to ping experiment. Failing ping is might be because of packet transmission is blocked or packet is discarded, while Traceroute uses an error message from a hop to find the route. Traceroute uses a trick to get the information, which is to manipulate the TTL (Time to Live), so the hop responds with an ICMP error (ICMP TTL exceeded).

Question 7:

a) The command '**arp -e**' is used to show the full ARP Table for any machine. The different columns in the arp table are:
(i) **Address**: This column represents the IP address of network connections which are present.
(ii) **Hwtype**: This represents the hardware type of this machine (here it is ethernet).
(iii) **Hwaddress**: This represents Mac Address (hardware address) to which IP is assigned.

(iv) **Flag**: Each complete entry in the ARP Cache will be marked with the C flag. Permanent entries are marked with M and published entries are marked with the P flag.
(v) **Mask:** This represents Genmask.
(vi) **Iface**: This represent network interface to which this address mapping has been assigned.

b) Adding : '**sudo arp -s IP_address mac_address**' : used to add a static ARP entry in ARP table with given ip and with given mac_address. Note that entries manually added have flag M. Another way to add IP addresses to the ARP table is by pinging to that IP address using the ping IP_address command.
Deleting : '**sudo arp –d IP_address**' : deletes the given IP from arp table. However, the entry would not be removed from the arp table after this command. This changes its hardware address to a sign of <incomplete> instead. Deleting things from caches is hard and expensive. Its way more efficient to invalidate an entry and wait if it is replaced before it is finally removed.

```
aryan@world-of-aryan:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp2s0
10.3.3.60                        (incomplete)                              enp2s0
192.168.1.1              ether   00:1e:a6:fb:64:d0   C                     enp2s0
aryan@world-of-aryan:~$ ping 10.3.3.35
PING 10.3.3.35 (10.3.3.35) 56(84) bytes of data.
From 10.3.3.61 icmp_seq=1 Destination Host Unreachable
From 10.3.3.61 icmp_seq=2 Destination Host Unreachable
From 10.3.3.61 icmp_seq=3 Destination Host Unreachable
From 10.3.3.61 icmp_seq=4 Destination Host Unreachable
From 10.3.3.61 icmp_seq=5 Destination Host Unreachable
From 10.3.3.61 icmp_seq=6 Destination Host Unreachable
^C
--- 10.3.3.35 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6147ms
pipe 4
aryan@world-of-aryan:~$ ping 10.3.3.34
PING 10.3.3.34 (10.3.3.34) 56(84) bytes of data.
64 bytes from 10.3.3.34: icmp_seq=1 ttl=64 time=0.556 ms
64 bytes from 10.3.3.34: icmp_seq=2 ttl=64 time=0.475 ms
64 bytes from 10.3.3.34: icmp_seq=3 ttl=64 time=0.298 ms
64 bytes from 10.3.3.34: icmp_seq=4 ttl=64 time=0.416 ms
64 bytes from 10.3.3.34: icmp_seq=5 ttl=64 time=0.425 ms
^C
--- 10.3.3.34 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4085ms
rtt min/avg/max/mdev = 0.298/0.434/0.556/0.084 ms
aryan@world-of-aryan:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp2s0
10.3.3.60                        (incomplete)                              enp2s0
10.3.3.34                ether   3c:52:82:3a:df:dd   C                     enp2s0
10.3.3.35                        (incomplete)                              enp2s0
192.168.1.1              ether   00:1e:a6:fb:64:d0   C                     enp2s0
```

Here just after executing ping 10.3.3.34 and 10.3.3.35, the IP address was found to be in the ARP table alongside three other IP addresses namely (10.3.3.34, 10.3.3.35, 10.3.3.60) which can be seen in the above picture.

c) The command **cat /proc/sys/net/ipv4/neigh/default/gc_stale_time** can be used to find how long entries in the cache of the ARP module of the kernel remain valid and get deleted from the cache.
Trial and Error Method: A linear guess solution can be used to guess the time after which an entry is deleted from the cache of the ARP module of the kernel. It works in a similar fashion to that of Binary Search. We can guess the time of deletion to be say 360 seconds, then make the system clock 360 seconds faster and look at what happens. Now try with 180 seconds if the ARP Cache has been cleared or try with 720 seconds if it has not been cleared. This way we can get an optimum solution by optimized Hit and Trial Method.

d) If two LANs on the same network have the map to the same Ethernet Address, it will confuse the switches. Any traffic sent to that IP address will be responded by both the LANs which will lead to a lot of confusion for the receiver primarily because both the devices have the same Ethernet Address. Each device will receive some of the frames destined for any one of them, which will be a complete mess.
A subnet is a smaller network created by dividing a larger network into equal parts. There are different hosts on a subnet. Different hosts on the same subnet are basically machines being plugged into the same set of hubs and switches. The machines talk to each other with their MAC Addresses which uniquely identifies each Ethernet/Wi-Fi/any other Network card. Each machine knows the IP address and not the MAC addresses. Let's say a host want to communicate with another host with IP Address "x". The first host then broadcasts a message in the network if some host knows the MAC address of any host with IP "x". Since, MAC Address of one host is unknown to another, only the target host responds back which indicates that the connection is established. One way to establish a connection using ping x command from the first machine.

Question 8:

Command used - ' **nmap -n -sP <Subnet Range>** '. Subnet range chosen: 172.16.112.0/26 itself.

Following data is obtained at different hours on 19.01.2020 among 64 hosts present:

Time (in 12 Hour format)	02:00 AM	06:00 AM	09:00 AM	01:00 PM	05:00 PM	08:00 PM
No. of Hosts online	9	2	9	26	30	28